**Nama : Maisy Rahmawati**

**NPM : 1806147035**

**Kelas : Jarkomdat - A**

**LOG WEEK 8**

**Materi: Network Layer DHCP**

* Network layer memiliki beberapa komponen yaitu DHCP, NAT, ICMP, Traceroute, IPv6. Komponen tersebut ada yang berada pada application layer. Komponen tersebut membantu dalam menentukan IP address dan mengalokasikan alamat. Device dapat memperoleh IP address melalui beberapa cara yaitu menggunakan static address dan dynamic address. Static address menyebabkan kita harus memasukkan IP address secara manual dan kita harus mengetahui subnettingnya. Dynamic address misalkan dengan DHCP melalui WiFi, maka IP address kita akan ditetapkan secara otomatis.
* IP address static dikelola oleh beberapa server (pemberi jasa layanan internet) karena IP address tersebut bersifat permanen dan biasanya server tersebut IP addressnya bersifat public sehingga dapat diakses oleh berbagai client.
* DHCP akan menyebabkan IP address yang berubah-ubah (dynamic). Biasanya cara DHCP digunakan oleh pengguna jasa layanan internet (client). DHCP memiliki tujuan untuk mendapatkan IP address secara dynamic dari network server ketika client (pengguna internet) bergabung di dalam network. Kriteria dari DHCP yaitu IP address bisa diperbaharui, IP address bisa digunakan kembali, dan dapat mendukung mobile users yang ingin bergabung di dalam network.
* DHCP lebih dari sekedar menetapkan IP address, tetapi juga dapat mengembalikan informasi lain yaitu address dari first hop router untuk client, name dan IP address dari DNS server, dan network mask (indicating network vs host portion of address). Router-router sederhana biasanya sudah memiliki DHCP server.
* DHCP overview:

1. Host broadcasts “DHCP discover” msg [optional]
2. DHCP server responds with “DHCP offer” msg [optional]
3. Host request IP address: “DHCP request” msg
4. DHCP server sends address: “DHCP ack” msg

* Contoh dari DHCP yaitu:

1. Router dengan DHCP server yang ada di dalam router tersebut digunakan untuk menetapkan IP address, address dari first-hop router, dan address dari DNS server untuk laptop yang terkoneksi.
2. DHCP request dienkapsulasi di dalam UDP. Lalu dienkapsulasi di Ethernet dan di-broadcast ke dalam semua jaringan sehingga DHCP server juga terkena broadcast-an tersebut.
3. Karena DHCP server pastinya juga terkena broadcast-an tersebut, maka DHCP server mengetahui bahwa terdapat client yang membutuhkan IP address sehingga DHCP akan melakukan offering kepada client (laptop).
4. Lalu client (laptop) melakukan request IP address kepada DHCP server. Lalu masuk ke network layernya.
5. DHCP akan memberikan kembali IP address tersebut sehingga client dapat mengetahui IP address, IP address dari first-hopnya, dan name dan IP address dari DNS server. Selanjutnya client akan menulisnya di dalam network interfacenya.

* Kita dapat memperoleh IP address dengan mengalokasikan portion dari ISP provider kita. ISP provider juga memberikan IP address public kepada kita yang selanjutnya kita gunakan sehingga kita dapat berselancar di dalam internet. Akan tetapi, ketika kita masuk ke dalam jaringan router kita, maka kita hanya diberikan IP address lokal.
* Organisasi yang mengatur block dari addresses adalah ICANN (Internet Corporation for Assigned Names and Numbers). ICANN akan mengalokasikan addresses, mengelola DNS, dan menetapkan domain names serta resolves jika terjadi disputes.

**Materi: Network Layer - NAT TraceRoute ICMP IPv6**

* NAT (Network Address Translation) berguna untuk mentranslate IP address yang diberikan oleh DHCP server agar client dapat berselancar di internet “seakan-akan” dia menggunakan IP address public.
* Semua datagram yang meninggalkan local network memiliki same single source NAT IP address (IP public).
* IP address public berguna untuk “mewakilkan” IP address local yang client miliki untuk dapat berselancar di internet. Misalkan client mengirimkan email melalui gmail, maka yang akan dikenali oleh gmail adalah IP address public yang diberikan oleh ISP provider sebagai wakil dari IP address local client. Ketika server akan mengirimkan data ke IP address local client maka harus dilakukan translate terlebih dahulu oleh NAT karena server tidak dapat mengenali IP address local client melainkan hanya mengenali IP address public yang diberikan oleh ISP provider yang client gunakan.
* Range address sangat jarang atau langka dari ISP artinya satu IP address (public) bersifat untuk semua device.
* Client dapat mengganti IP address di dalam local networknya secara dinamis sebanyak subnetting yang ia miliki.
* Device di dalam local network secara eksplisit tidak dapat diakses dari luar sehingga perlu adanya translate menggunakan NAT.
* NAT router harus:

1. Outgoing datagram: replace
2. Remember (pada NAT translation table)
3. Incoming datagram: replace

* ICMP (Internet Control Message Protocol) sebagai suatu protokol yang digunakan agar client dapat mengontrol atau mengetahui status dari message yang dimilikinya. ICMP digunakan oleh hosts dan routers untuk saling berkomunikasi pada network level information untuk mengetahui error reporting dan echo request atau reply. ICMP message dikirim atau dibawa menggunakan IP datagram. ICMP juga merupakan salah satu contoh application layer sama seperti DHCP. Namun, ICMP lebih digunakan untuk mengontrol atau mengetahui status message pada network layer.
* Traceroute digunakan untuk mengetahui status dari tempat client ke suatu server, jumlah hoping, dan waktu yang diperlukan untuk berpindah dari satu hop ke hop lain (dihitung dengan menggunakan TTL). Ketika ICMP message sampai maka source akan merecord RTTs. Stopping criteria terjadi jika UDP segment telah sampai ke destination host, jumlah hop-nya dibatasi atau “port unreachable”.
* IPv6 merupakan salah satu solusi ketika terjadi keterbatasan 32 bit address pada IPv4. IPv6 mempunyai fixed-length sebesar 40 byte header dan tidak ada fragmentasi yang diizinkan.
* Datagram format pada IPv6 terdiri dari priority, flow label, dan next header.
* IPv6 memiliki source address dan destination address sebesar 128 bits (sebagai pembeda dari IPv4).
* Beberapa hal yang berubah dari IPv4 ke IPv6 yaitu checksum yang dihapus karena dapat mengurangi waktu setiap kali berada di hop. Selain itu, ada pula versi baru ICMP yaitu ICMPv6, serta options yang diizinkan namun diluar dari header.
* Tunneling merupakan solusi agar IPv4 dapat berjalan hingga saat ini, di mana datagram IPv6 dibawa sebagai muatan dalam datagram IPv4 di antara router IPv4 karena network antara router belum semuanya dapat berganti menjadi IPv6 sehingga IPv6 dibungkus terlebih dahulu di dalam datagram IPv4.

**Materi : Routing in the Internet (RIP, OSPF, BGP)**

* Intra-AS Routing atau Interior Gateway Protocols (IGP) secara umum terdiri dari RIP (Routing Information Protocol), OSPF (Open Shortest Path First), dan IGRP (Interior Gateway Routing Protocol / Cisco Proprietary).
* RIP (Routing Information Protocol) termasuk dalam distribusi BSD-UNIX pada tahun 1982. Di dalam protokol ini, terdapat algoritma yang digunakan untuk menentukan gateway yang disebut dengan distance vector algorithm (decentralized). Terdapat beberapa ketentuan di dalam distance vector algorithm yaitu distance metric yaitu
* Jumlah hops (# hops) dengan maksimal terdapat 15 hops, di mana setiap link memiliki cost l.
* DVs bertukar dengan neighbors setiap 30 detik melalui response message atau disebut juga advertisement.
* Setiap advertisement yaitu merupakan daftar hingga 25 destination subnets (di dalam arti IP addressing).
* Pada RIP, jika tidak terdapat advertisement yang terdengar setelah 180 detik maka neighbor atau link akan dinyatakan mati. Beberapa hal diantaranya karena rute melalui neighbor invalidated, terdapat new advertisement yang mengirim ke neighbor, neighbor berada dalam pengiriman new advertisement (jika table berubah), dan adanya info link failure dengan cepat menyebar ke seluruh jaringan.
* OSPF (Open Shortest Path First) merupakan protokol yang menggunakan link state algorithm (centralized) dengan penyebaran LS packet, topologi map pada setiap node, dan perhitungan rute menggunakan Dijkstra’s algorithm. OSPF advertisements membawa satu entri untuk setiap neighbor. Advertisements dibawa dalam pesan OSPF langsung melalui IP (bukan TCP atau UDP).
* Hierarchical OSPF diantaranya:
* Two-level hierarchy → bersifat local area, backbone.

Di dalam hierarchy ini, link-state advertisements hanya berada di dalam local area. Setiap node memiliki detail area topology yang hanya mengetahui arah dari nets di area lainnya.

* Area border routers → merupakan “ringkasan” jarak ke nets di dalam area sendiri dan mengirimkan advertisement ke routers perbatasan area lainnya.
* Backbone routers → menjalankan OSPF routing yang terbatas pada backbone.
* Boundary routers → menghubungkan ke AS’s lainnya.
* BGP (Border Gateway Protocol) adalah de facto inter-domain routing protocol atau “glue yang menyatukan internet. BGP menyediakan suatu sarana untuk setiap AS yaitu eBGP dan iBGP. eBGP mendapatkan informasi jangkauan subnet dari AS’s neighbor. Sedangkan iBGP menyebarkan informasi jangkauan ke semua router internal AS. BGP menentukan rute yang "baik" ke jaringan lain berdasarkan informasi dan kebijakan jangkauan. BGP memungkinkan subnet untuk mengiklankan keberadaannya ke seluruh internet lainnya.
* BGP session terdiri dari dua router BGP yang bertukar BGP message: jalur advertising ke prefiks jaringan tujuan yang berbeda dan bertukar melalui koneksi TCP semi permanen.
* Ketika router learns terhadap new prefix, maka akan dibuat entry untuk prefix tersebut di dalam forwarding tablenya.
* BGP router selection di mana router mungkin mempelajari tentang lebih dari bagaimana ia akan memberikan rute ke destination AS, memilih rute berdasarkan

1. Local preference value attribute: policy decision
2. Shortest AS-PATH
3. Closest NEXT-HOP router: hot potato routing
4. Additional criteria